

instrumentalities of a conspiracy to commit robbery, in violation of Title 18, United States Code, Section 1951(a); robbery, in violation of Title 18, United States Code, Section 1951(a); conspiracy to commit interstate transportation of stolen property, in violation of Title 18, United States Code, Sections 371 and 2314; and interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314.

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the DEA. I have been employed by the DEA for approximately 14 years. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for narcotics crimes and other violent crimes, including robbery. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, (b) reports made to me by other law enforcement authorities, (c) information obtained from confidential sources of information, (d) information obtained from interviews with witnesses and victims, and (e) review of other records and reports.

3. The DEA is investigating a conspiracy to interfere with commerce by robbery and a conspiracy to commit interstate transportation of stolen property, as well as related substantive offenses.

I. BACKGROUND

4. On or about December 22, 2009, three individuals entered a residence at 1767 East 7th Street, Brooklyn, New York (the "East 7th Street Residence"), by force through the rear door. The robbers were armed with screwdrivers. Once inside the residence, the robbers subdued multiple victims, two of whom were minors. While inside the residence, the robbers stole approximately \$5,000 cash and property valued at approximately \$250,000, including jewelry, electronics belonging to a business, autographed sports memorabilia, and clothing. After leaving the East 7th Street Residence, the robbers stole a black 2010 Ferrari California automobile, which belonged to one of the victims and

was parked outside the residence.

5. A cooperating witness ("CW") was arrested for his/her role in the robbery. The information provided by the CW has been corroborated by independent evidence and proven reliable. The CW told agents, among other things, that KENNETH DAVIS and JERMAN VERDUGO participated in the afore-mentioned robbery as well as numerous others. The CW further told agents, among other things, that a co-conspirator, DERRICK DIAZ, would transport the property obtained from the robberies from New York to his home in New Jersey, and then back to New York for re-sale on the black market.

6. On September 22, 2010, DEA special agents arrested VERDUGO at his residence in Roselle Park, New Jersey, for his participation in the aforementioned offenses.

7. On November 16, 2010, DEA special agents arrested DAVIS at his residence in Brooklyn, New York, for his participation in the aforementioned offenses.

8. On November 30, 2011, VERDUGO pleaded guilty to interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314, in United States v. Derrick Diaz et al., 10 CR 277 (S-4) (KAM).

9. DAVIS and co-defendant DERRICK DIAZ are charged in a superseding indictment with conspiracy to commit robbery from December 2007 to January 2010, in violation of Title 18, United

States Code, Section 1951(a); robbery, in violation of Title 18, United States Code, Section 1951(a); conspiracy to commit interstate transportation of stolen property, in violation of Title 18, United States Code, Sections 371 and 2314; and interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314. Trial is scheduled to commence on February 21, 2012 before the Hon. Kiyo A. Matsumoto.

II. TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than

by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such

as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. Electronic mail: Electronic mail, commonly called email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If a sender or recipient of the message does not delete the message, the message can remain on the device

indefinitely. If an email user writes a draft message but does not send it, that message may also be saved on the device but may not include all of these categories of data. The DEVICE can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails on the device, and attachments to emails, including pictures and files.

i. Text Messages: Text messaging, or texting, refers to the exchange of brief written text messages between fixed-line phone or mobile phone and fixed or portable devices over a network, and included messages which contain image, video, and sound content.

j. Facebook/MySpace: Facebook and MySpace are a social networking services and websites. Users of these sites may create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profile. Users must register before using the site. Users can create profiles with photos, lists of personal interests, contact information, and other personal information. Users can communicate with friends and other users through private or public messages and a chat feature. Users can access and store personal information, such as contacts, telephone numbers, and photographs on their accounts.

11. Based on my training, experience, and the investigation thus far, I know that the DEVICES (the seizure of which is described below in paragraphs 12-14) have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, and are capable of using Facebook/MySpace and other similar programs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICES.

III. THE DEVICES

12. At the time of VERDUGO's arrest, the Motorola mobile telephone and the iPhone were seized from VERDUGO. The Motorola mobile telephone and the iPhone are currently being kept in the custody of the DEA and the U.S. Attorney's Office in the Eastern District of New York.

13. At the time of DAVIS's arrest, the Blackberry was seized from DAVIS. The Blackberry is currently being kept in the custody of the DEA and the U.S. Attorney's Office in the Eastern District of New York.

14. The CW has told agents that the members of the conspiracy, including DAVIS and VERDUGO, communicated amongst themselves by telephone to set up and arrange robberies and to arrange to receive their shares of the proceeds when the stolen goods were sold.

15. Telephone records, obtained by subpoena, have revealed substantial telephone contacts between the members of the conspiracy, including DAVIS and VERDUGO, during the time period of the conspiracy.

16. Based on my knowledge, training, and experience, I know that the DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the Devices. This information can sometimes be recovered with forensics tools.

IV. TECHNICAL BACKGROUND

17. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the DEVICES because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the

electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

18. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence

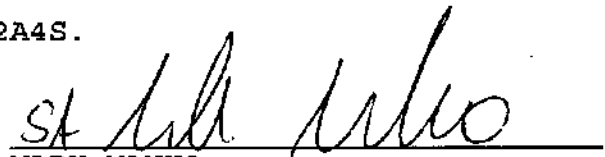
described by the warrant.

19. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto the Devices. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.


V. CONCLUSION

20. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the DEVICES there exists evidence of crimes. Accordingly, a search warrant is requested.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS: (1) A BLACK BLACKBERRY CURVE, ESN 80179D18; (2) A MAROON MOTOROLA i880, IMEI 001700669938710; AND (3) A BLACK APPLE IPHONE, SERIAL NUMBER 87030PZ2A4S.


MARK MANKO
Special Agent
Drug Enforcement Administration

Sworn to before me this
6th day of February, 2012



THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The property to be searched is: (1) A BLACK BLACKBERRY CURVE, ESN 80179D18; (2) A MAROON MOTOROLA i880, IMEI 001700669938710; AND (3) A BLACK APPLE IPHONE, SERIAL NUMBER 87030PZ2A4S; hereinafter the "Devices." This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
Particular Things to be Seized

All information obtained from Devices will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes fruits, evidence and instrumentalities of conspiracy to commit robbery, in violation of Title 18, United States Code, Section 1951(a); robbery, in violation of Title 18, United States Code, Section 1951(a); conspiracy to commit interstate transportation of stolen property, in violation of Title 18, United States Code, Sections 371 and 2314; and interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314, including:

1. All records and information on the Devices described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of conspiracy to commit robbery, in violation of Title 18, United States Code, Section 1951(a); robbery, in violation of Title 18, United States Code, Section 1951(a); conspiracy to commit interstate transportation of stolen property, in violation of Title 18, United States Code, Sections 371 and 2314; and interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314;
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
4. Evidence of the lack of such malicious software;
5. Evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data)

that are designed to eliminate data from the Devices;

7. Evidence of the times the Devices were used;
8. Passwords, encryption keys, and other access devices that may be necessary to access the Devices; and
9. Contextual information necessary to understand the evidence described in this attachment,

all of which constitute evidence, fruits and instrumentalities of conspiracy to commit robbery, in violation of Title 18, United States Code, Section 1951(a); robbery, in violation of Title 18, United States Code, Section 1951(a); conspiracy to commit interstate transportation of stolen property, in violation of Title 18, United States Code, Sections 371 and 2314; and interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.